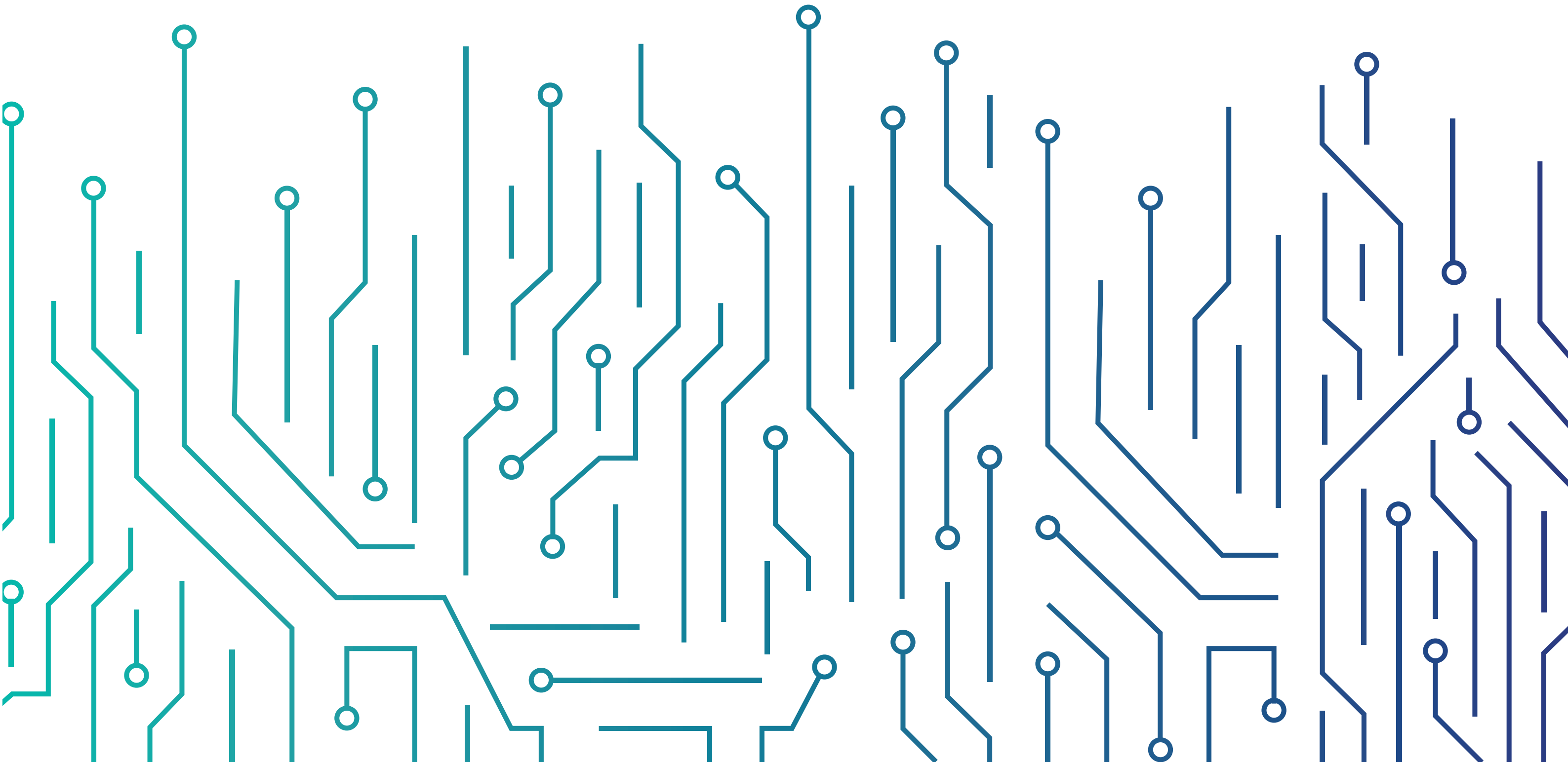
الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Telework Cybersecurity Controls

(TCC -1:2021)

Sharing Notice: White
Document Classification: Open



Disclaimer: The following controls will be governed by and implemented in accordance with the laws of the Kingdom of Saudi Arabia, and must be subject to the exclusive jurisdiction of the courts of the Kingdom of Saudi Arabia. Therefore, the Arabic version will be the binding language for all matters relating to the meaning or interpretation of this document.

In the Name of Allah,
The Most Gracious,
The Most Merciful

Traffic Light Protocol (TLP):

This marking protocol is widely used around the world. It has four colors (traffic lights):

🔴 **Red – Personal and Confidential to the Recipient only**

The recipient is not allowed to share red-classified materials with any person, from within or outside the institution, beyond the scope specified for receipt.

🟠 **Amber – Limited Sharing**

The recipient of amber-classified materials may share the information contained therein with concerned personnel only in the same institution, and with those competent to take procedures with regard to the information.

🟢 **Green – Sharing within the Same Community**

Green-classified materials may be shared with others within the same institution or in other institutions that have relations with your institution or are operating in the same sector. However, such materials may not be shared or exchanged through public channels.

⚪ **White – No Restrictions**

Table Of Contents

List of Tables

List of The Figures and Illustrations

Executive Summary

With the continuous technical advancements that coincide with developments in the workforce market, flexible technical options are available to enable a remote work environment. This technology enables employees to perform many functions and tasks without the need to be physically present in the workplace. This contributes to promoting economic development and new job opportunities, as well as increasing productivity and performance. There is no doubt that the increasing dependence of some entities on telework increases threats and cyber risks to telework systems, which requires setting cybersecurity requirements to reduce these threats and risks.

Under the Royal Decree number 6801, dated 11/2/1439 H, The National Cybersecurity Authority has become the sole authority in the Kingdom of Saudi Arabia for cybersecurity, and the National Reference in its affairs. These include development, update and dissemination of policies, governance mechanisms, frameworks, cybersecurity standards, controls and guidelines to national organisations as well as monierting their compliance. Thereby enhancing the role of cybersecurity and its importance; and the urgent need for it that has increased with the rapid increase of threats and cyber risks more than Ever.

NCA's mandate states that its responsibility for cybersecurity does not absolve any public, private or other organization from its own cybersecurity responsibilities as confirmed by the Royal Decree number 57231, dated 10/11/1439 H, which states that "all government organizations must improve their cybersecurity level to protect their networks, systems and data, and comply with NCA's policies, framework, standards, controls and guidelines"

From this national perspective towards teleworking, with the purpose to achieve a secure and reliable Saudi cyber space enabling growth and prosperity, the NCA developed the Telework Cybersecurity Controls (TCC-1: 2021) to set the minimum cybersecurity requirements to enable national organizations to perform telework in a secure manner, in addition to the Essential Cybersecurity Controls (ECC-1:2018). This document highlights the details of these controls, goals, scope, statement of applicability, compliance approach and monitoring, taking into consideration, Critical Systems Cybersecurity Controls (CSCC – 1:2019) in cases where critical systems are used in telework.

All national organizations must implement all necessary measures to ensure continuous compliance with the TCC as per item 3 of article 10 of NCA's mandate and as per the Royal Decree number 57231, dated 10/11/1439H.

Introduction

In today's world, the work environment is witnessing many changes due to the impact of modern technologies. The acceleration of emerging technologies such as artificial intelligence and virtual reality are increasing the partnership between man and technology. Among other things, this convergence is leading to the further development of the concept of telework that is significantly reducing the links between geography and the actual work being performed.

Because of these changes, the Kingdom has started to move towards enhancing flexibility in work-place to enable business to perform remotely to achieve a number of economic, development and security goals in accordance with the Kingdom's Vision 2030. This type of telework requires the presence of cybersecurity controls that are aimed at helping businesses and consumers avoid and mitigate cyber threats and to resolved them with minimal impact on the vital interests of the state, its national security, sensitive infrastructure, priority sectors, government services and activities.

The National Cybersecurity Authority (referred to in this document as "The Authority" or "NCA") developed the Telework Cybersecurity Controls (TCC – 1: 2021) after:

- Conducting a comprehensive study of multiple national and international cybersecurity frameworks and standards.
- Studying related national decisions, law and regulatory requirements.
- Reviewing and leveraging cybersecurity best practices.
- Analyzing previous cybersecurity incidents and attacks on government and other critical organizations.
- Surveying and considering opinions of multiple national organizations.

The NCA has aligned the TCC with the ECC. Compliance with the ECC is a prerequisite for the TCC. Continuous compliance with both is required to be compliant with the relevant national, international and legislative, regulatory requirements. The Telework Cybersecurity Controls consist of the following:

- 3 Main Domains
- 16 Subdomains
- 21 Main Controls
- 42 Subcontrols

Objectives

The Telework Cybersecurity Controls aim to:

- Enabling an organization's work to be performed remotely in a secure manner and adapt to the changes in the business environment and in telework systems.
- Enhancing the organization's cybersecurity capabilities and resilience in cases where telework is exposed to cyber threats that could result in negative impacts and costly losses.
- Contributing to raising the level of cybersecurity at the national level.

Scope of Work and Applicability

TCC Scope of Work

These controls are applicable to government organizations in the Kingdom of Saudi Arabia including ministries, authorities, establishments and others and companies and entities, as well as private sector organizations owning, operating or hosting Critical National Infrastructure (CNIs), which are all referred to herein as "The Organization".

The NCA strongly encourages all other organizations in the Kingdom to leverage these controls to implement these best practices to improve and enhance their cybersecurity.

TCC Scope of Work

These controls have been developed after taking into consideration the cybersecurity needs of all organizations and sectors in the Kingdom of Saudi Arabia. Every organization that allows telework must comply with all applicable controls in this document.

Applicability to implement these cybersecurity controls depends on the organization's business and its use of certain technologies. For example:

- Controls in subdomain 3-1 (Cloud Computing and Hosting Cybersecurity) are applicable and must be implemented by organizations currently using or planning to use cloud computing and hosting services.

Implementation and Compliance

To comply with item 3 of article 10 of NCA's mandate and as per the Royal Decree number 57231 dated 10/11/1439H, all organizations within the scope of these controls must implement whatever is necessary to ensure continuous compliance with the controls. This can only be accomplished by achieving continuous compliance with the ECC (ECC – 1:2018) where applicable.

NCA evaluates organizations' compliance with the TCC through multiple means such as self-assessments by the organizations, and/or External Compliance Assessment.

Update and Review

NCA will periodically review and update the TCC as per the cybersecurity requirements and related industry updates. NCA will communicate and publish the updated version of TCC for implementation and compliance.

TCC Domains and Structure

Main domains and subdomains of TCC

The following figure shows the main domains and subdomains of the Telework Cybersecurity Controls (TCC). Appendix (A) clarifies the relationship with the Essential Cybersecurity Controls (ECC).

1- Cybersecurity Governance	1-1	Cybersecurity Policies and Procedures	1-2	Cybersecurity Risk Management
	1-3	Cybersecurity Awareness and Training Program		
2- Cybersecurity Defense	2-1	Asset Management	2-2	Identity and Access Management
	2-3	Information System and Processing Facilities Protection	2-4	Networks Security Management
	2-5	Mobile Devices Security	2-6	Data and Information Protection
	2-7	Cryptography	2-8	Backup and Recovery Management
	2-9	Vulnerabilities Management	2-10	Penetration Testing
	2-11	Cybersecurity Event Logs and Monitoring Management	2-12	(Cybersecurity Incident and Threat Management)
3- Third-Party and Cloud Computing Cybersecurity	3-1	Cloud Computing and Hosting Cybersecurity		

Figure (1): TCC Domains and Subdomains

Structure

Figure (2) and (3) below show the meaning of controls codes:

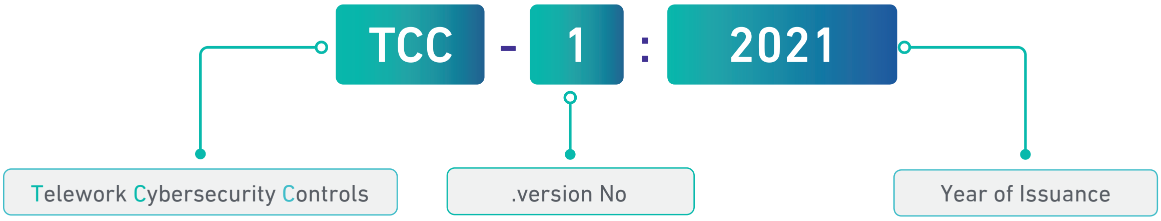


Figure (2): Controls Coding Scheme

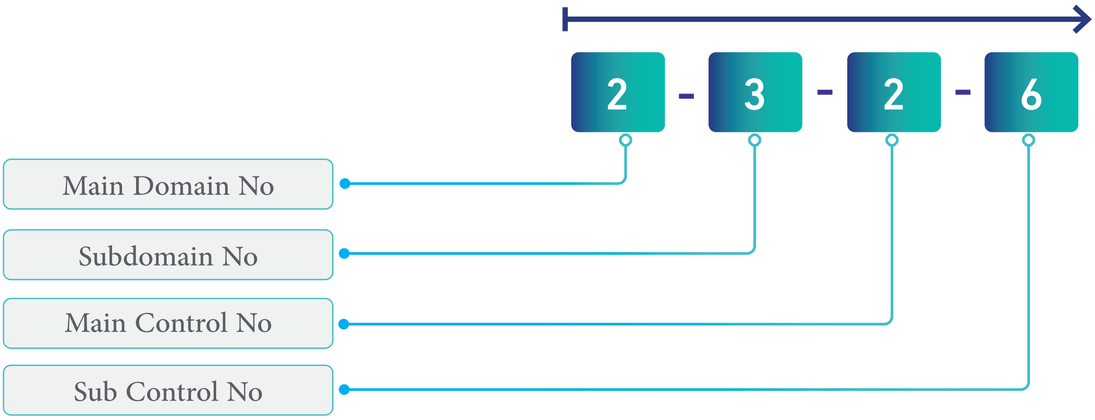


Figure (3): TCC Structure

Please note that the green colored numbers (such as: 1-3-1), are reference numbers to related ECC subdomain or control.

Table (1) below shows the methodological structure of the controls:

1	Name of Main Domain
Reference number of the Main Domain	
Reference number of the Subdomain	Name of Subdomain
Objective	
Controls	
Reference number of the control	Control clauses

Table (1): TCC Structure

Telework Cybersecurity Controls

1 Cybersecurity Governance

1-1	Cybersecurity Policies and Procedures
Objective	To ensure that cybersecurity requirements are documented, communicated and complied with by the organization as per related laws and regulations, and organizational requirements.
Controls	
1-1-1	Referring to control 1-3-1 in the ECC, cybersecurity policies and procedures must include the following: 1-1-1-1 Defining and documenting the telework cybersecurity requirements and controls as part of the organization's cybersecurity policies.
1-2	Cybersecurity Risk Management
Objective	To ensure managing cybersecurity risks in a methodological approach in order to protect the organization's information and technology assets as per organizational policies and procedures, and related laws and regulations.
Controls	
1-2-1	In addition to the controls within subdomain 1-5 in the ECC, requirements for cybersecurity risk management should include at least the following: 1-2-1-1 Assessment of the cybersecurity risks for telework systems, once per year at least. 1-2-1-2 Assessment of cybersecurity risks during planning and before permitting telework for any service or system. 1-2-1-3 Including the cybersecurity risks related to telework systems and its related services and systems in the entity's cybersecurity risk register, and monitoring it at least once a year.

1-3	Cybersecurity Awareness and Training Program
Objective	To ensure that personnel are aware of their cybersecurity responsibilities and have the essential cybersecurity awareness. It is also to ensure that personnel are provided with the required cybersecurity training, skills and credentials needed to accomplish their cybersecurity responsibilities and to protect the organization's information and technology assets.
Controls	
1-3-1	In addition to the sub-controls within control 1-10-3 in the ECC, the cybersecurity awareness program must cover the awareness about the potential cyber risks and threats related to telework, including the following: 1-3-1-1 Secure use of telework devices and how to protect them. 1-3-1-2 Secure handling of identities and passwords. 1-3-1-3 Protection of the stored data on the telework devices, and to be handled based on its classification. 1-3-1-4 Secure handling of applications and solutions used for telework such as: virtual conferencing and collaboration, and file sharing solutions. 1-3-1-5 Secure handling of home networks, making sure it is configured in a secure way. 1-3-1-6 Avoidance of teleworking using unreliable public devices or networks or while in public places. 1-3-1-7 Unauthorized physical access, loss, theft, and sabotage of technical assets and telework systems. 1-3-1-8 To Communicate directly with the cybersecurity department If a cybersecurity threat is suspected.
1-3-2	In addition to the sub-controls within control 1-10-4 in the ECC, employees must be trained with the required technical skills to ensure the implementation of the cybersecurity requirements when handling telework systems.

2 Cybersecurity Defense

2-1	Asset Management
Objective	To ensure that the organization has an accurate and detailed inventory of information and technology assets in order to support the organization’s cybersecurity and operational requirements to maintain the confidentiality, integrity and availability of information and technology assets.
Controls	
2-1-1	In addition to the controls within subdomain 2-1 in the ECC, cybersecurity requirements for asset management related to telework systems should include at least the following: 2-1-1-1 Identifying and maintaining an annually-updated Inventory of information and technology assets of the telework systems.
2-2	Identity and Access Management
Objective	To ensure the secure and restricted logical access to information and technology assets in order to prevent unauthorized access and allow only authorized access for users which are necessary to accomplish assigned tasks.
Controls	
2-2-1	In addition to the sub-controls within control 2-2-3 in the ECC, cybersecurity requirements for identity and access management related to telework systems shall include at least the following: 2-2-1-1 Managing telework access rights based on need, considering the sensitivity of the systems, the level of access rights and the type of devices used by employees for telework. 2-2-1-2 Restricting remote access for the same user from multiple computers at the same time (Concurrent Logins). 2-2-1-3 Using secure standards to manage identities and passwords used in the telework systems.
2-2-2	With reference to the ECC subcontrol 2-2-3-5, user’s identities and access rights used for telework must be reviewed at least once every year.

2-3	Information System and Processing Facilities Protection
Objective	To ensure the protection of information systems and information processing facilities (including workstations and infrastructures) against cyber risks.
Controls	
2-3-1	In addition to the subcontrols in the ECC control 2-3-3, cybersecurity requirements for protecting telework systems and information processing facilities must include at least the following: 2-3-1-1 Applying updates and security patches for telework systems at least once every three months. 2-3-1-2 Reviewing telework systems' configurations and hardening at least once every year. 2-3-1-3 Reviewing and changing default configurations, and ensuring the removal of hard-coded, backdoor and/or default passwords. 2-3-1-4 Securing Session Management which includes the session authenticity, lockout, and timeout. 2-3-1-5 Restricting the activation of the features and services of the telework systems based on needs, provided that potential cyber risks are analyzed in case there is a need to activate them.
2-4	Network Security Management
Objective	To ensure the protection of organization's network from cyber risks.
Controls	
2-4-1	In addition to the subcontrols in the ECC control 2-5-3, cybersecurity requirements of telework systems' network security management must include at least the following: 2-4-1-1 Restrictions on network services, protocols and ports used to access remotely, specifically to internal systems and to only be opened based on need. 2-4-1-2 Reviewing firewall rules and configurations, at least once every year. 2-4-1-3 Protecting against Distributed Denial of Service Attack (DDoS) attacks to limit risks arising from these attacks. 2-4-1-4 Protecting against Advanced Persistent Threats (APT) at the network layer.
2-5	Mobile Device Security
Objective	To ensure the protection of mobile devices (including laptops, smartphones, tablets) from cyber risks and to ensure the secure handling of the organization's information (including sensitive information) while utilizing Bring Your Own Device (BYOD) policy.
Controls	
2-5-1	In addition to the sub-controls within control 2-6-3 in the ECC, cybersecurity requirements for mobile device security related to telework systems shall include at least the following: 2-5-1-1 Central management of mobile devices and BYODs using a Mobile Device Management system (MDM). 2-5-1-2 Applying updates and security patches on mobile devices, at least once every month.

2-6	Data and Information Protection
Objective	To ensure the confidentiality, integrity and availability of organization's data and information as per organizational policies and procedures, and related laws and regulations.
Controls	
2-6-1	In addition to the subcontrols in the ECC control 2-7-3, cybersecurity requirements for protecting and handling data and information must include at least the following: 2-6-1-1 Identifying classified data, according to the relevant regulations, that can be used, accessed or dealt with through telework systems. 2-6-1-2 Protecting classified data, which was identified in control 2-6-1-1, using controls such as: not allowing the use of a specific type of classified data, or by the use of technology (e.g. Data leakage Prevention), such controls and technologies can be determined by analyzing the cyber risks of the organization.
2-7	Cryptography
Objective	In addition to the sub-controls within control 2-8-3 in the ECC, cybersecurity requirements for cryptography related to telework systems shall include at least the following:
Controls	
2-7-1	In addition to the sub-controls within control 2-8-3 in the ECC, cybersecurity requirements for cryptography related to telework systems shall include at least the following: 2-7-1-1 The use of updated and secure methods and algorithms for encryption over the entire network connection used for telework, according to the Advanced level within the National Cryptography Standards (NCS 1:2020).
2-8	Backup and Recovery Management
Objective	To ensure the protection of organization's data and information including information systems and software configurations from cyber risks as per organizational policies and procedures, and related laws and regulations.
Controls	
2-8-1	In addition to the subcontrols in the ECC control 2-9-3, cybersecurity requirements for backup and recovery management must include at least the following: 2-8-1-1 Performing backup within planned intervals, according to the organization's risk assessment.
2-8-2	With reference to the ECC subcontrol 2-9-3-3, a periodical test must be conducted at least once every six months in order to determine the efficiency of recovering telework systems backups.

2-9	Vulnerabilities Management
Objective	To ensure timely detection and effective remediation of technical vulnerabilities to prevent or minimize the probability of exploiting these vulnerabilities to launch cyber attacks against the organization.
Controls	
2-9-1	In addition to the subcontrols in the ECC control 2-10-3, cybersecurity requirements for technical vulnerabilities management of telework systems must include at least the following: 2-9-1-1 Assessing vulnerabilities on technical components of telework systems, and to be classified based on criticality at least once every three months. 2-9-1-2 Remediating vulnerabilities for telework systems, at least once every three months.
2-10	Penetration Testing
Objective	To assess and evaluate the efficiency of the organization’s cybersecurity defense capabilities through simulated cyber-attacks to discover unknown weaknesses within the technical infrastructure that may lead to a cyber breach.
Controls	
2-10-1	In addition to the sub-controls within control 2-11-3 in the ECC, cybersecurity requirements for penetration testing related to telework systems shall include at least the following: 2-10-1-1 Scope of penetration tests must cover all of the telework systems’ technical components.
2-10-2	With reference to the ECC subcontrol 2-11-3-2, penetration tests must be conducted on telework systems at least once every year.
2-11	Cybersecurity Events Logs and Monitoring Management
Objective	To ensure timely collection, analysis and monitoring of cybersecurity events for early detection of potential cyber-attacks in order to prevent or minimize the negative impacts on the organization’s operations.
Controls	
2-11-1	In addition to the subcontrols in the ECC control 2-12-3, cybersecurity requirements for event logs and monitoring management for telework systems must include at least the following: 2-11-1-1 Activating cybersecurity events logs on all technical components of telework systems. 2-11-1-2 Monitoring and analyzing user behavior (UBA). 2-11-1-3 Monitoring telework systems events around the clock. 2-11-1-4 Updating and implementing cybersecurity monitoring procedures around the clock, to include monitoring remote access operations, especially remote access from outside the Kingdom of Saudi Arabia, after checking their authenticity.

2-11-2	With reference to the ECC subcontrol 2-12-3-5, retention period of cybersecurity's telework systems event logs must be 12 months minimum, in accordance with relevant legislative and regulatory requirements.
2-12	Cybersecurity Incident and Threat Management
Objective	To ensure timely identification, detection, effective management and handling of cybersecurity incidents and threats to prevent or minimize negative impacts on organization's operation taking into consideration the Royal Decree number 37140, dated 14/8/1438H.
Controls	
2-12-1	In addition to the sub-controls within control 2-13-3 in the ECC, cybersecurity requirements for incident and threat management related to telework systems shall include at least the following: 2-12-1-1 Updating cyber security incidents response plans and contact information within the organization in a way that is compatible with the telework situation and to ensure the ability to communicate and the preparedness of the incident response teams. 2-12-1-2 Periodically obtaining and dealing with threat intelligence information related to telework systems. 2-12-1-3 Addressing and implementing the recommendations and alerts for cyber security incidents and threats issued by the Sector regulator or by the National Cybersecurity Authority (NCA).

3 Third Party And Cloud Computing Cybersecurity

3-1	Cloud Computing and Hosting Cybersecurity
Objective	To ensure the proper and efficient remediation of cyber risks and the implementation of cybersecurity requirements related to hosting and cloud computing as per organizational policies and procedures, and related laws and regulations. It is also to ensure the protection of the organization’s information and technology assets hosted on the cloud or processed/ managed by third-parties.
Controls	
3-1-1	In addition to the subcontrols in the ECC control 4-2-3, cybersecurity requirements related to the use of hosting and cloud computing services must include at least the following: 3-1-1-1 The location of the hosted telework systems must be inside the Kingdom of Saudi Arabia.

Appendices

Appendix (A): The relationship with the Essential Cybersecurity Controls

Telework Cybersecurity Controls (TCC – 1: 2021) is an extension to Essential Cybersecurity Controls (ECC- 1: 2018) as illustrated in figures (4) & (5), whereas the following items are added:

- Cybersecurity controls for telework are added to sixteen subdomains.
- There are no telework cybersecurity controls added to thirteen subdomains.

🟦	Subdomains where cybersecurity controls have been added for organizations' highly sensitive social media accounts
⬜	Subdomains where no additional cybersecurity controls have been added for organizations› highly sensitive social media accounts

Figure 4. Guide to Colors of Subdomains in Figure 5

<table>
<tr><td rowspan="5">1- Cybersecurity Governance</td><td colspan="2">Cybersecurity Strategy</td><td colspan="2">Cybersecurity Management</td></tr>
<tr><td>1-1</td><td>Cybersecurity Policies and Procedures</td><td colspan="2">Cybersecurity Roles and Responsibilities</td></tr>
<tr><td>1-2</td><td>Cybersecurity Risk Management</td><td colspan="2">Cybersecurity in Information Technology Projects</td></tr>
<tr><td colspan="2">Cybersecurity Regulatory Compliance</td><td colspan="2">Cybersecurity Periodical Assessment and Audit</td></tr>
<tr><td colspan="2">Cybersecurity in Human Resources</td><td>1-3</td><td>Cybersecurity Awareness and Training Program</td></tr>
<tr><td rowspan="8">2- Cybersecurity Defense</td><td>2-1</td><td>Asset Management</td><td>2-2</td><td>Identity and Access Management</td></tr>
<tr><td>2-3</td><td>Information System and Processing Facilities Protection</td><td colspan="2">Email Protection</td></tr>
<tr><td>2-4</td><td>Networks Security Management</td><td>2-5</td><td>Mobile Devices Security</td></tr>
<tr><td>2-6</td><td>Data and Information Protection</td><td>2-7</td><td>Cryptography</td></tr>
<tr><td>2-8</td><td>Backup and Recovery Management</td><td>2-9</td><td>Vulnerabilities Management</td></tr>
<tr><td>2-10</td><td>Penetration Testing</td><td>2-11</td><td>Cybersecurity Event Logs and Monitoring Management</td></tr>
<tr><td>2-12</td><td>Cybersecurity Incident and Threat Management</td><td colspan="2">Physical Security</td></tr>
<tr><td colspan="4">Web Application Security</td></tr>
<tr><td>3- Cybersecurity Resilience</td><td colspan="4">Cybersecurity Resilience aspects of Business Continuity Management (BCM)</td></tr>
<tr><td>4- Third party Cybersecurity</td><td colspan="2">Third-Party Cybersecurity</td><td>4-1</td><td>Cloud Computing and Hosting Cybersecurity</td></tr>
<tr><td>5 - ICS Cybersecurity</td><td colspan="4">Industrial Control Systems (ICS) Protection</td></tr>
</table>

Figure 5. ECC and TCC subdomains

Appendix (B): Terms and Definitions

Table (2) below highlights some of the terms and their definitions which were used in this document.

Terminology	Definition
Telework Systems	It is any technical systems, means or tools and its related components which are used by the organization to enable employees to perform their job duties in a place other than the official workplace. Examples include: virtual meeting systems, collaboration systems, file sharing, virtual private network (VPN), remote access systems, and other systems used in the work environment.
User Behavior Analytics (UBA)	It is the process of tracking and collecting user data. Analyze it, and define patterns of user activity; to detect harmful or unusual behaviors.
Data Leakage Prevention	Technologies used to protect sensitive data from unauthorized disclosure, and to prevent its circulation outside the organization in any form of such data, and its location; whether stored on volumes (At-rest), or on the user devices or servers (In-Use), or in movement via the network (In-transit).
Distributed Denial of Service Attack (DDoS)	It is an attempt to disable the system and make its services unavailable by sending many requests from more than one source at the same time.
Mobile Device Management (MDM) System	It is a technical system used to manage, monitor, and protect mobile devices by applying cybersecurity policies.

Table (2): Terms and Definitions

Appendix (C): List of Abbreviations

Table (3) below shows some of the abbreviations and their meanings which are used in this document.

Abb.	Full Term
APT	Advanced Persistent Threat.
BCM	Business Continuity Management
BYOD	Bring Your Own Device
ECC	Essential Cybersecurity Controls
ICS	Industrial Control Systems
TLP	Traffic Light Protocol

Table (3): List of Abbreviations

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority